(1)

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 03-239032

(43)Date of publication of application : 24.10.1991

(51)Int.Cl. H04K 1/00
H04N 7/167

(21)Application number : 02-035723

(22)Date of filing : 16.02.1990

(71)Applicant : SONY CORP

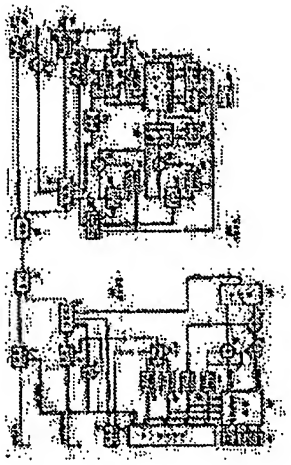
(72)Inventor : HOSHINO TAKANARI
YAMASHITA MASAMI
OSADA YASUO

(54) RECEIVER FOR SCRAMBLE SIGNAL

(57)Abstract:

PURPOSE: To prevent interception resulting from forgery of a reception signal by extracting a data signal for preventing forgery inserted in plural positions in the received signal, comparing them mutually and applying descrambling only when they are coincident.

CONSTITUTION: A format of a common information signal string consists of a header ID representing common information, key signals K1, K2 in 16-bit each, key signals K3, K4 in 32-bit each, a 4-bit forgery preventing ID, and a 4-bit channel number or the like, and with a 24-bit error correction code at the end in total 256 bits. The forgery preventing ID provided to a data of the common information signal string and a data of an individual information signal string in a memory 37 is read by a dissidence detection circuit 40 in a timing from a generating circuit 30 and when dissidence is detected, the content of the memory 37 is reset and all channels are brought into the uncontracted state. Thus, the interception is inhibited in an excellent way.



When the descrambling operation is authorized, key signals K_4 and K_2 from the memory (37) are supplied as initial values to random-signal generating circuits (41) and (42), and a frame synchronous signal from the separating circuit (24) is detected by a detecting circuit (43) to be supplied to the generating circuits (41) and (42). A random signal thus generated is selected by a switch (44) to be supplied to the descrambling circuit (25) and the subtracter (27). A flag (identification signal) indicating a switching state of the switch is supplied to a switching-signal generating circuit (45). Switching of the switch (44) is controlled based on a signal from the generating circuit (45).

The video signal and the PCM audio signal thus received are descrambled.

In the scrambled-signal receiving apparatus, for example, each of a common-information signal string and an individual-information signal string has tampering prevention ID on a transmission side, and the ID is extracted to be compared with another on the reception side. When non-matching is determined, the data written in the memory (37) is reset, and an operation such as authorization of the descrambling operation based on the data is prohibited.

That is, for example, even when the contractor extracts the individual-information signal string by using a computer in an all-channel contracted state, and inserts, after annulment of the contract, the extracted individual-information signal into a received signal to tamper, non-matching occurs at a point of time when the tampering prevention ID of the common-information signal string is changed, and authorization of the descrambling operation is

prohibited. This results in high security against interceptions and tapping.

⑲日本国特許庁(JP)　⑪特許出願公開

⑫公開特許公報(A)　平3−239032

⑤Int. Cl.⁵	識別記号	庁内整理番号	⑬公開　平成3年(1991)10月24日
H 04 K 1/00	Z	6914−5K	
H 04 N 7/167		8943−5C	

審査請求　未請求　請求項の数 2　(全7頁)

⑤発明の名称　スクランブル信号の受信装置

⑳特　願　平2−35723
㉒出　願　平2(1990)2月16日

⑦発明者　星野　隆也　東京都品川区北品川6丁目7番35号　ソニー株式会社内
⑦発明者　山下　雅美　東京都品川区北品川6丁目7番35号　ソニー株式会社内
⑦発明者　長田　保夫　東京都品川区北品川6丁目7番35号　ソニー株式会社内
⑦出願人　ソニー株式会社　東京都品川区北品川6丁目7番35号
⑦代理人　弁理士　松隈　秀盛

明　細　書

発明の名称　スクランブル信号の受信装置

特許請求の範囲

1. スクランブルされた信号と、上記スクランブル用のキー信号と、受信登録番号信号と、時間的に異なる複数箇所に挿入された改ざん防止用のデータ信号とを含む送信信号を受信する装置であって、

上記受信登録番号信号を抽出し自己の登録番号と比較して一致を検出すると共に、

上記複数箇所に挿入された改ざん防止用のデータ信号を抽出し相互比較して一致を検出し、

これらが共に一致を検出した時に上記スクランブルされた信号のデスクランブル動作を行うようにしたスクランブル信号の受信装置。

2. 少くとも第1及び第2の改ざん防止用のデータ信号が設けられ、

受信登録番号信号と上記第1の改ざん防止用のデータ信号が個別情報信号列に挿入され、

スクランブル用のキー信号と上記第2の改ざん防止用のデータ信号が共通情報信号列に挿入され、

上記第1及び第2の改ざん防止用のデータ信号を抽出し一致を検出するようにした上記特許請求の範囲第1項記載のスクランブル信号の受信装置。

発明の詳細な説明

以下の順序で本発明を説明する。

A　産業上の利用分野
B　発明の概要
C　従来の技術
D　発明が解決しようとする課題
E　課題を解決するための手段
F　作用
G　実施例
H　発明の効果

A　産業上の利用分野

本発明は、例えばテレビジョン信号を通信衛星を用いて送信する場合に使用されるスクランブル

信号の受信装置に関する。

B　発明の概要

本発明はスクランブル信号の受信装置に関し、受信信号中の複数箇所に挿入された改ざん防止用のデータ信号を抽出し、これらを相互に比較して一致したときのみデスクランブル動作を行うことによって、受信信号の改ざんによる盗視聴を良好に禁止できるようにしたものである。

C　従来の技術

例えば通信衛星を用いてテレビジョン信号の送信を行う場合に、非契約者の盗視聴を禁止する目的で信号をスクランブルすることが考えられている。

その場合に、映像信号のスクランブルについては、例えば特開昭60－256286～8 号公報に示されるような、いわゆるラインシャフリングの技術が提案されている。

D　発明が解決しようとする課題

ところで、上述のような例えば通信衛星を用いたテレビジョン信号の送信においては、複数のチャンネルが設けられると共に、そのチャンネルごとに受信契約を結ぶことが考えられている。その場合に契約者は例えば１ヶ月単位で契約チャンネルを変更する可能性があり、その際に一々契約者の所へ出向いて受信装置の切替等を行うのは極めて困難である。

そこで送信信号中に各契約者の契約チャンネル等の個別情報を挿入し、受信装置はこの個別情報を検出して装置を自動切替することが考えられた。

しかしながらこのような自動切替を行っている場合に、例えば全チャンネルを契約した契約者が契約期間中に上述の個別情報を含む情報信号を抽出し、契約終了後にこの抽出した情報信号を受信信号に混入する改ざんを行うことによって、契約していないチャンネルを盗視聴できることが判明した。

この出願はこのような点に鑑みてなされたもので、簡単な構成で上述の改ざんによる盗視聴を良好に禁止できるようにしたものである。

E　課題を解決するための手段

本発明による第１の手段は、スクランブルされた信号と、上記スクランブル用のキー信号（K_1～K_n）と、受信登録番号（加入者データ）信号と、時間的に異なる複数箇所に挿入された改ざん防止用のデータ（改ざん防止用ＩＤ）信号とを含む送信信号を受信する装置(200) であって、上記受信登録番号信号を抽出し自己の登録番号（デコーダ識別番号）と比較して一致を検出（オーソライズ回路(38)）すると共に、上記複数箇所に挿入された改ざん防止用のデータ信号を抽出し相互比較して一致を検出（不一致検出回路(40)）し、これらが共に一致を検出した時に上記スクランブルされた信号のデスクランブル動作を行うようにしたスクランブル信号の受信装置である。

第２の手段は、少くとも第１及び第２の改ざん防止用のデータ（改ざん防止用ＩＤ）信号が設けられ、受信登録番号（加入者データ）信号と上記第１の改ざん防止用のデータ信号が個別情報信号列（第２図Ｂ）に挿入され、スクランブル用のキー信号（K_1～K_n）と上記第２の改ざん防止用のデータ信号が共通情報信号列（第２図Ａ）に挿入され、上記第１及び第２の改ざん防止用のデータ信号を抽出し一致を検出（不一致検出回路(40)）するようにした上記第１の手段記載のスクランブル信号の受信装置である。

F　作用

これによれば、受信信号中の複数箇所に挿入された改ざん防止用のデータ信号を抽出し、これらを相互比較して一致した時のみデスクランブル動作が行われるので、受信信号の改ざんによる盗視聴を良好に禁止することができ、簡単な構成で良好なスクランブル信号の受信を行うことができる。

G　実施例

第１図は送信から受信までのシステム構成を示

し、図中(100)は送信側の装置、(200)は受信側の装置をそれぞれ全体として示している。

この図において、(1)は映像信号の入力端子であって、この入力端子(1)からの映像信号が上述のラインシャフリング等のスクランブル回路(2)に供給され、スクランブルされた映像信号が送信回路(3)に供給される。また(4)は音声信号の入力端子であって、この音声信号は例えば48kHz でサンプリングされ16ビットで量子化されたＰＣＭ音声信号が供給される。この入力端子(4)からの音声信号がスクランブル回路(5)に供給されて、任意のビット反転等のスクランブルが行われ、このスクランブルされた音声信号が多重化回路(6)を通じて送信回路(3)に供給される。

さらに(7)はキー信号発生回路であって、この発生回路(7)からの時々刻々変化される所定のキー信号K_3が映像信号のスクランブル用のデータ（ＳＤＡ）としてスクランブル回路(2)に供給される。それと共にこのキー信号K_3(ーＳＤＡ）が加算器（イクスクルーシブオア回路）(8)に供給されて、任意のビット反転等のスクランブルが行われ、このスクランブルされたキー信号K_3が多重化回路(6)に供給される。

また発生回路(7)からのキー信号K_1, K_2がそれぞれＭ系列等のランダム信号発生回路(9)(10)に初期値として供給され、これらの発生回路(9)(10)からのランダム信号がスイッチ(11)で選択されて、音声信号のスクランブル回路(5)及び加算器(8)に供給される。なおキー信号K_1, K_2はスイッチ(11)で選択されていない間に順次値が変更される。これによって音声信号及びキー信号K_3のスクランブルが行われる。

さらにスイッチ(11)の切替が切替信号発生回路(12)からの信号で制御されると共に、この切替状態を示すフラグ（識別信号）が多重化回路(6)に供給される。なおこの切替は後述するキー信号K_3, K_4の伝送に対して余裕を持った間隔で行われる。

また(13)はそれぞれ情報データの発生手段であって、例えばコンピュータからなるこの発生手段(13)では、チャンネル番号等の放送データ、各契約者の加入者番号及び契約チャンネル番号等の個別情報を含む加入者データ（受信登録番号）、改ざん防止用ＩＤ、誤り訂正コード等が発生される。この発生手段 (13)からの情報データが情報信号列形成回路(14)に供給される。さらに上述の発生回路(7)からのキー信号K_1, K_2及び後述のK_3, K_4が形成回路(14)に供給される。

そしてこの形成回路(14)では、例えば次に述べるような２つのフォーマットで情報信号列が形成される。すなわち第２図Ａは共通情報信号列のフォーマットを示し、時系列の先頭（左）側から例えば８ビットの後続が共通情報であることを示すヘッダＩＤ、それぞれ16ビットのキー信号K_1, K_2、それぞれ32ビットのキー信号K_3, K_4、４ビットの改ざん防止用ＩＤ、４ビットのチャンネル番号等が設けられ、末尾に24ビットの誤り訂正コードが設けられて全体が 256ビットにされている。また同図Ｂは個別情報信号列のフォーマットを示し、同じく時系列の先頭（左）側から例えば８ビットの後続が個別情報であることを示すヘッダＩＤ、22ビットの加入者番号、４ビットの改ざん防止ＩＤ、192ビットの各契約者個別情報等が設けられ、末尾に24ビットの誤り訂正コードが設けられて全体が256 ビットにされている。

この共通情報信号列及び個別情報信号列がそれぞれ加算器（イクスクルーシブオア回路）(15)(16)に供給される。さらに発生回路(7)からのキー信号K_1がランダム信号発生回路(17)に初期値として供給され、この発生回路(17)からのランダム信号が加算器(15)(16)に供給される。この加算器(16)からの信号が加算器(18)に供給されると共に、発生回路(7)からのキー信号K_2がランダム信号発生回路(19)に初期値として供給され、この発生回路(19)からのランダム信号が加算器(18)に供給される。

これによって共通情報信号列にはキー信号K_1によるスクランブルが行われ、個別情報信号列にはキー信号K_1及びK_2によるスクランブルが行われる。なお実際には、共通情報信号列ではヘッダとキー信号K_1を除くキー信号K_2以降にキー

信号K₁によるスクランブルが行われ、個別情報信号列ではヘッダを除く部分にキー信号K₁及びK₂によるスクランブルが行われている。またこれらのキー信号K₁及びK₂は例えば5秒ごとに順次値が変化されている。

これらのスクランブルされた共通情報信号列及び個別情報信号列が多重化回路(20)に供給され、例えば個別情報信号列が9回に共通情報信号列が1回の割合で、時分割多重化される。この多重化された信号が多重化回路(6)に供給される。

そしてこの多重化回路(6)では、例えば次に述べたような多重化が行われる。すなわちこの装置においては、PCM音声信号はいわゆる放送衛星におけるBモード音声に準拠した形式で伝送が行われている。そこで第3図は1ms周期で伝送される1フレームのビットインターリーブマトリクスを示しており、このマトリクスは32行64列で構成される。ここで第1列，第2列はフレーム同期、音声信号のモード等を示す制御符号及びレンジビットのエリアとされ、続く第3列～第50列がPCM音声信号のエリアとされる。さらに第58列～第64列が誤り訂正コードのエリアとされると共に、これらの間の第51列～第57列はBモード音声では独立データエリアとされている。

従って上述の多重化回路(6)においてはこの第51列～第57列のエリアにスクランブルされたキー信号K₂、スイッチ(11)の切替状態を示すフラグ及び共通情報信号列または個別情報信号列を多重化することができる。なお共通情報信号列及び個別情報信号列は、例えば各フレームに8ビットずつ伝送され、全体は32フレームかけて伝送される。そして上述のようにスクランブルされた映像信号と、スクランブル及び多重化された音声信号が送信回路(3)に供給され、例えば通信衛星（図示せず）を用いて受信側の装置(200)に伝送される。

そこでこの受信側の装置(200)において、まず受信回路(21)で受信された映像信号がデスクランブル回路(22)に供給され、上述のラインシャフリングが元に戻されて出力端子(23)に取出される。また受信回路(21)で受信された音声信号が分離回路(24)を通じてデスクランブル回路(25)に供給され、任意のビット反転等が元に戻されて出力端子(26)に取出される。

さらに分離回路(24)にて、キー信号K₂に相当する信号が分離され、この信号が減算器（イクスクルーシブオア回路）(27)に供給されて、任意のビット反転等のデスクランブルが行われる。このデスクランブルによって復元されたキー信号K₂（＝SDA）がデスクランブル回路(22)に供給される。

また分離回路(24)にて上述の共通情報信号列及び個別情報信号列に相当する信号が分離され、この信号が減算器(28)とキー信号K₁のメモリ(29)に供給される。それと共に分離回路(24)からの信号がヘッダ検出及びタイミング発生回路(30)に供給され、この発生回路(30)からの共通情報のヘッダIDが検出された直後のキー信号K₁の期間に相当する信号がメモリ(29)に供給されて、キー信号K₁がメモリ(29)に書込まれる。さらにこのメモリ(29)に書込まれたキー信号K₁がランダム信号発生回路(31)に初期値として供給されると共に、発生回路(30)からの共通情報のヘッダIDが検出されたときのキー信号K₂以降の期間及び個別情報のヘッダIDが検出されたときの加入者番号以降の期間に相当する信号が発生回路(31)に供給され、この期間に発生されたランダム信号が減算器(28)に供給される。これによって共通情報信号列のキー信号K₂以降の信号のデスクランブルが行われる。

この減算器(28)からの信号が減算器(32)とキー信号K₂のメモリ(33)に供給される。それと共に発生回路(30)からの共通情報のヘッダIDが検出された後のキー信号K₂の期間に相当する信号がメモリ(33)に供給されて、キー信号K₂がメモリ(33)に書込まれる。このメモリ(33)に書込まれたキー信号K₂がランダム信号発生回路(34)に初期値として供給されると共に、発生回路(30)からの個別情報のヘッダIDが検出されたときの加入者番号以降の期間に相当する信号が発生回路(34)に供給され、この期間に発生されたランダム信号が

減算器(32)に供給される。これによって個別情報信号列の加入者番号以降の信号のデスクランブルが行われる。

この減算器(32)からの信号がデータラッチ及び誤り訂正の回路(メモリ)(35)に供給される。一方発生回路(30)からの信号がメモリ制御回路(36)に供給され、この制御回路(36)からの信号が回路(35)に供給される。これによって、上述のキー信号K_3,K_4、改ざん防止ＩＤ、チャンネル番号、加入者番号、改ざん防止ＩＤ、各契約者個別情報等のデータがそれぞれ回路(35)にラッチされる。

さらにこの回路(35)にて各情報信号列の末尾の誤り訂正コードを用いてデータの誤り訂正が行われる。そしてこの誤り訂正が終了し、データの誤りが無くなったときにそれを示す信号が制御回路(36)に供給され、この制御回路(36)からの信号がメモリ(37)に供給されて、回路(35)にラッチされた各データがメモリ(37)に転送される。

これによって各データがメモリ(37)に書込まれる。そこでこれらのデータに対して、まず加入者番号が発生回路(30)からの所定のタイミングでオーソライズ回路(38)に読出される。一方このオーソライズ回路(38)には受信装置(200)ごとに独立に設けられたデコーダ識別番号（登録番号）がその記憶手段(39)から供給され、この識別番号と上述の加入者番号（受信登録番号）とが比較され、これらが一致したときに以降の各契約者個別情報が有効とされて、ここに設けられた契約チャンネル番号等の情報が抽出保存される。そして共通情報信号列中のチャンネル番号と契約チャンネル番号とが一致したときに、デスクランブル動作の承認が行われる。またメモリ(37)の共通情報信号列のデータと個別情報信号列のデータのそれぞれに設けられた改ざん防止ＩＤが発生回路(30)からのタイミングで不一致検出回路(40)に読出され、不一致が検出されたときにメモリ(37)の内容がリセットされて全チャンネルが未契約の状態となるようにされる。

そして上述のデスクランブル動作の承認が行われたときは、メモリ(37)からのキー信号K_1,K_2がそれぞれランダム信号発生回路(41)(42)に初期値として供給され、また分離回路(24)からのフレーム同期信号が検出回路(43)で検出されて発生回路(41)(42)に供給される。これによって発生されたランダム信号がスイッチ(44)で選択されてデスクランブル回路(25)、減算器(27)に供給されると共に、分離回路(24)からのスイッチの切替状態を示すフラグ（識別信号）が切替信号発生回路(45)に供給され、この発生回路(45)からの信号でスイッチ(44)の切替が制御される。

このようにして受信された映像信号及びＰＣＭ音声信号のデスクランブルが行われる。

そしてさらにこの装置においては、例えば送信側で共通情報信号列と個別情報信号列のそれぞれに改ざん防止ＩＤが設けられ、受信側でこれらを抽出し相互比較してこれが不一致になった時にメモリ(37)に書込まれたデータがリセットされ、これによるデスクランブル動作の承認等の動作が禁止される。

すなわち上述の装置において、例えば契約者が全チャンネルを契約した状態でコンピュータ等を用いて個別情報信号列を抽出し、契約解除後にこの抽出した個別情報信号を受信信号に挿入して改ざんを行っても、共通情報信号列の改ざん防止用ＩＤが変更された時点で不一致となり、デスクランブル動作の承認が禁止される。これによって盗視聴を良好に禁止することができるものである。

なお改ざん防止用ＩＤのみを改ざんすることは極めて困難である。また共通情報信号列も抽出して、これも一緒に改ざんすることは、キー信号が変化されるのでデスクランブルの意味がなくなる。

さらに雑音等により、正規の受信であるのに改ざん防止用ＩＤが誤るおそれがあるが、通常このような誤りは誤り訂正回路(35)で訂正されるか除去される。また万一誤って通過された場合には、不一致検出回路(40)が複数回連続して検出されたときに検出を判断するように設定することによって、誤動作を確実に防止することができる。

従って上述の装置によれば、受信信号中の複数箇所に挿入された改ざん防止用のデータ信号を抽

出し、これらを相互比較して一致した時のみデスクランブル動作が行われるので、受信信号の改ざんによる盗視聴を良好に禁止することができ、簡単な構成で良好なスクランブル信号の受信を行うことができるものである。

なお上述の装置において、キー信号K_1,K_2を任意に切替えてスクランブルを行うことによって無断の解読を極めて困難にしている。

またキー信号K_1でスクランブルされた情報の中に個別情報信号列のスクランブルのキー信号K_2を設けることによって個別情報信号列の機密性を極めて高くしている。

さらにデスクランブルの承認を個別情報信号列をデスクランブルするデータが検出されるまで禁止することによって、誤動作の発生を良好に防止している。

またデスクランブルされたデータを一旦ラッチし、誤りが無いときのみメモリに転送することによって誤動作のおそれを大幅に減少させている。

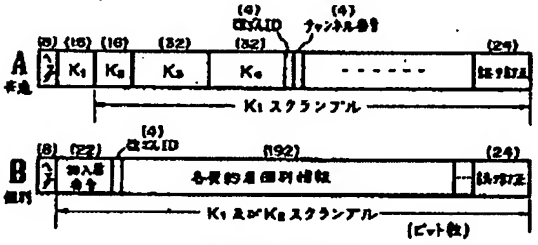
H 発明の効果

この発明によれば、受信信号中の複数箇所に挿入された改ざん防止用のデータ信号を抽出し、これらを相互比較して一致した時のみデスクランブル動作が行われるので、受信信号の改ざんによる盗視聴を良好に禁止することができ、簡単な構成で良好なスクランブル信号の受信を行うことができるようになった。

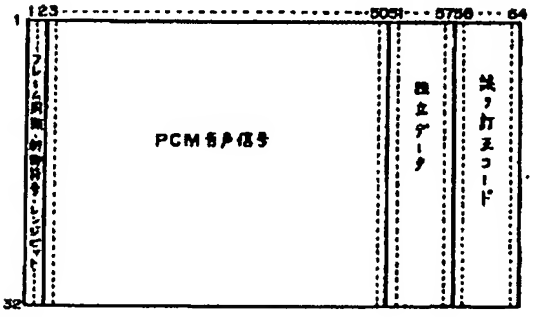
図面の簡単な説明

第1図は本発明によるスクランブル信号の受信装置を含む全体のシステムの一例の構成図、第2図は伝送される情報信号列のフォーマットを示す線図、第3図はＰＣＭ音声信号のビットインターリーブマトリクスを示す線図である。

(1)(4)は入力端子、(2)(5)はスクランブル回路、(3)は送信回路、(6)(20)は多重化回路、(7)はキー信号発生回路、(8)(15)(16)(18)は加算器、(9)(10)(17)(19)(31)(34)(41)(42)はランダム信号発生回路、(11)(44)はスイッチ、(12)(45)は切替信号発生回路、(13)は情報データ発生回路、(14)は情報信号列形成回路、(21)は受信回路、(22)(25)はデスクランブル回路、(23)(26)は出力端子、(24)は分離回路、(27)(28)(32)は減算器、(29)(33)(37)はメモリ、(30)はヘッダ検出及びタイミング発生回路、(35)はデータラッチ及び誤り訂正回路、(36)はメモリ制御回路、(38)はオーソライズ回路、(39)は識別番号の記憶手段、(40)は不一致検出回路、(43)は同期検出回路、(100)は送信装置、(200)は受信装置である。

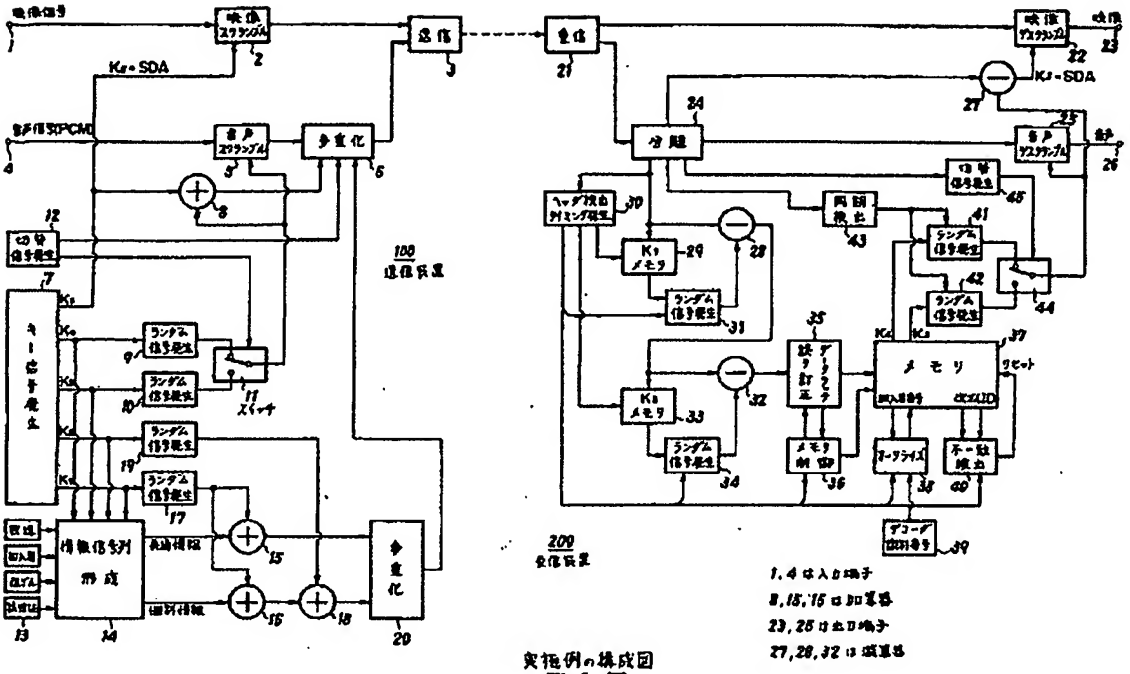


情報信号列フォーマット
第 2 図



ビットインターリーアマトリクス
第 3 図

代 理 人　　松 隈 秀 盛


Ka・SDA
Kb・SDA
100
送信装置
200
受信装置
スイッチ
1, 4 は入力端子
8, 15, 16 は加算器
23, 25 は出力端子
27, 28, 32 は減算器

実施例の構成図
第 1 図